DE 3915262 (1)
H04L9/000-H04L9/008-

H04L 9/08

-2- * -

(19) [redacted]2 A1

(51) Int. Cl. 4:
G 09 C 5/00
H 04 L 9/00

DEUTSCHES
PATENTAMT

(21) Aktenzeichen: P 39 15 262.6
(22) Anmeldetag: 10. 5. 89
(43) Offenlegungstag: 30. 11. 89

DE 3915262 A1

(30) Unionspriorität: (32) (33) (31)
18.05.88 CH 1877/88

(71) Anmelder:
Asea Brown Boveri AG, Baden, Aargau, CH

(74) Vertreter:
Rupprecht, K., Dipl.-Ing., Pat.-Anw., 6242 Kronberg

(72) Erfinder:
Günther, Christoph, Dipl.-Phys. Dr., Fislisbach, CH

DOC

(54) Verfahren zur Erzeugung von authentifizierten Geheimschlüsseln

Bei einem Verfahren zur Erzeugung von authentifizierten Geheimschlüsseln werden bei einer Präauthentifikation und einem nachfolgenden Schlüsselaufbau dieselben mathematischen Rechenoperationen eingesetzt. Für die Präauthentifikation der Teilnehmer A und B wählt jeder Teilnehmer einen endlichen Körper GF(p) (resp. GF(q)), ein Element α (resp. β) aus dem endlichen Körper GF(p) (resp. GF(q)) und eine erste geheime Zufallszahl

$\{\hat{x} \in 0..p-2\}$ (resp. $\{\hat{y} \in 0..q-2\}$).

Dann erzeugt er einen Authentifikationsschlüssel

$\alpha^{\hat{x}}$ (resp. $\beta^{\hat{y}}$),

indem er sein Element α (resp. β) mit seiner ersten geheimen Zufallszahl

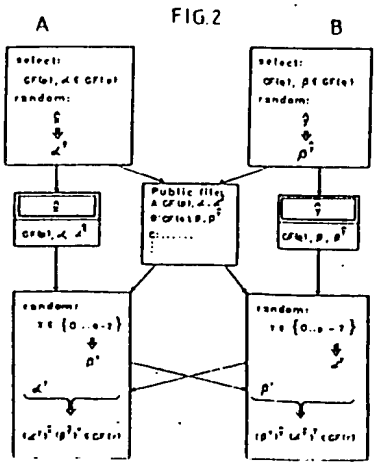
$\hat{x}$ (resp. $\hat{y}$)

potenziert, und gibt diesen zusammen mit dem endlichen Körper GF(p) (resp. GF(q)) und dem Element α (resp. β) in authentifizierter Weise öffentlich bekannt. Beim Schlüsselaufbau gehen die beiden Teilnehmer A und B so vor, daß jeder der beiden Teilnehmer A (resp. B) eine zweite geheime Zufallszahl $[x \in 0 .. q-2]$ (resp. $[y \in 0 .. p-2]$) und einen Betriebsschlüssel β^x (resp. α^y) erzeugt, indem er das Element β beiden Teilnehmer A und B die Größen β^x und α^y austauschen und den gemeinsamen authentifizierten Geheimschlüssel

$\alpha^{\hat{x}y} \cdot \beta^{\hat{y}x}$

berechnen.

FIG.2



DE 3915262 A1

Beschreibung

Technisches Gebiet

Die Erfindung beschreibt ein Verfahren zur Erzeugung von authentifizierten Geheimschlüsseln.

Stand der Technik

Zum authentifizierten Schlüsselaustausch sind im wesentlichen die folgenden Verfahren bekannt

- Authentifikation eines zufällig erzeugten Schlüssels durch die Sprache, z. B. CH-Patentanmeldung Nr. 4307/87-0
- Authentifikation eines zufällig erzeugten Schlüssels durch elektronische Signaturen:
  a) mit einem symmetrischen Chiffrieralgorithmus,
  b) mit dem RSA Verfahren (siehe R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Comm. of the ACM, Vol. 21, pp. 120—126, 1978)
  c) mit dem El-Gamal Verfahren (siehe T. El-Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. on Information Theory, Vol. IT-31, pp. 469—471, July 1985),
  d) Schlüsselaustausch mit dem Diffie-Hellman Verfahren (siehe W. Diffie, M. Hellman, "New directions in Cryptography", IEEE Trans. on Information Theory, Vol. IT-22, pp. 472—492, 1976).

Allen Verfahren ist gemeinsam, daß sie eine Präauthentifikation benötigen. Dies ist überhaupt eine Eigenschaft aller Authentifikationsverfahren und beruht darauf, daß es unmöglich ist jemanden zu identifizieren, den man nicht entweder bereits kennt oder von dem man nicht über eine vertrauenswürdige Quelle weiß, wer er ist. Eine mögliche Form der Präauthentifikation ist, daß jeder Teilnehmer zu einer Schlüsselauthentifikationszentrale geht, sich mit seinem Reisepaß ausweist, ein eigenes Merkmal hinterlegt und ein entsprechendes Merkmal der Zentrale mitnimmt. Im Fall von mehreren Zentralen müssen auch diese untereinander in entsprechender Weise vorgehen. Die Merkmale die benutzt werden, sind dabei vom verwendeten Verfahren abhängig.

Die verschiedenen Verfahren unterscheiden sich in zweierlei Hinsicht, in ihrer Benutzerfreundlichkeit und der durch sie gewährten Sicherheit.

- Die Authentifikation durch die Sprache ist bei gewissen Anwendungen nur bedingt benutzerfreundlich.
- Die Signatur mit einem symmetrischen Chiffrieralgorithmus hat den Nachteil, daß, wenn der sowohl beim Teilnehmer als auch in der Zentrale bekannte geheime Authentifikationsschlüssel bekannt wird, die gesamte Kommunikation, die mit diesem Schlüssel authentifiziert wurde, nachträglich dechiffriert werden kann.
- Ähnlich, aber bereits etwas weniger schlimm, verhält es sich bei den publizierten Signaturen, d. h., beim RSA- und El-Gamal-Verfahren: Wenn der geheime Dechiffrierschlüssel des Teilnehmers A, der bei diesem Verfahren nur noch im Besitz dieses Teilnehmers ist, bekannt wird, können alle Datenübertragungen, die unter diesem Schlüssel jemals beim Teilnehmer A eingegangen, d. h., von außen initialisiert worden sind, dechiffriert werden. Durch eine geringfügige Ausdehnung dieses Verfahrens läßt sich erreichen, daß die geheimen Dechiffrierschlüssel beider Teilnehmer bekannt werden müssen, damit obige Situation eintreten kann. Ein weiterer Nachteil des RSA-Verfahrens liegt schließlich in der komplizierten Erzeugung der RSA-Schlüssel.
- das Diffie-Hellman Verfahren hat schließlich den Nachteil, daß zwischen zwei gleichen Teilnehmern stets der gleiche Schlüssel vermerkt wird, was zu einer ähnlichen Situation wie beim RSA-Verfahren führt.

Darstellung der Erfindung

Aufgabe der Erfindung ist es entsprechend ein Verfahren zur Erzeugung von authentifizierten (und geheimen) Schlüsseln anzugeben, das nur zwischen den gewünschten Teilnehmern zum Erfolg führt (Authentifikation) und außerdem bei einer erneuten Schlüsselerzeugung im allgemeinen zu anderen Schlüsseln führt.

Erfindungsgemäß besteht die Lösung darin, daß der Teilnehmer A (resp. B) in einer Präauthentifikationsphase, ähnlich wie beim Diffie-Hellman Verfahren, die folgenden Schritte durchführt:

P1) Der Teilnehmer A (resp. B) wählt einen geeigneten endlichen Körper $GF(p)$ (resp. $GF(q)$) und ein geeignetes Element $\alpha \varepsilon\, GF(p)$ (resp. $\beta \varepsilon\, GF(q)$). Außerdem wählt er zufällig eine Zahl $\hat{x} \varepsilon\, 0 \ldots p-2$ (resp. $\hat{y} \varepsilon\, 0 \ldots q-2$) die er für immer geheim hält.
P2) Er bildet $\alpha^{\hat{x}}$ (resp. $\beta^{\hat{y}}$) und gibt diesen zusammen mit $GF(p)$ und α (resp. mit $GF(q)$ und β) in authentifizierter Weise bekannt, z. B. indem er sie in einer Authentifikationszentrale hinterlegt.

Durch diese vorbereiteten Schritte können nun die Teilnehmer A und B zu jedem Zeitpunkt über eine insbesondere nicht abhörgeschützte Verbindung einen authentifizierten nur von einem bekannten Schlüssel wie folgt konstruieren:

S1. Die Teilnehmer A und B verschaffen sich die Authentifikationsmerkmale $(GF(q), \beta, \beta^{\hat{y}})$ und $(GF(p), \alpha, \alpha^{\hat{x}})$ ihrer Partner B und A.
S2. Die Teilnehmer A und B wählen zufällig eine zweite Zahl $\{x \varepsilon\, 0 \ldots q-2\}$, $\{y \varepsilon\, 0 \ldots p-2\}$, die sie wieder für immer geheim halten.
S3. Sie bilden die Größen β^x und α^y und tauschen diese aus.
S4. Teilnehmer A bildet die Größe

$$(\alpha^y)^{\hat{x}} (\beta^{\hat{y}})^x = \alpha^{\hat{x}y} \beta^{x\hat{y}}$$

im kleinsten Erweiterungskörper der $GF(p)$ und $GF(q)$ enthält und Teilnehmer B bildet im gleichen Körper die Größe

$$(\alpha^{\hat{x}})^y (\beta^x)^{\hat{y}} = \alpha^{\hat{x}y} \beta^{x\hat{y}}.$$

Diese gemeinsame Größe, die, sofern das Diffie-Hellman Verfahren sicher ist, nur sie kennen können, verwenden sie als gemeinsamen Schlüssel.

In einer bevorzugten Ausführungsform verwenden A und B denselben endlichen Körper $GF(p)$ und dasselbe Element. In diesem Fall lautet der Geheimschlüssel

$\alpha^{\xi y + x\eta}$

Kurze Beschreibung der Zeichnungen

Nachfolgnd soll die Erfindung anhand von Ausführungsbeispielen und im Zusammenhang mit den Zeichnungen näher erläutert werden. Es zeigen:

Fig. 1 ein Verschlüsselungsgerät, welches nach dem erfindungsgemäßen Verfahren arbeitet, und

Fig. 2 eine schematische Darstellung des erfindungsgemäßen Verfahrens.

Wege zur Ausführung der Erfindung

Fig. 1 zeigt eine Ausführungsform eines Chiffriergeräts **12**, welches nach dem erfindungsgemäßen Verfahren arbeitet.

An einem Datenanschluß **1**, wo z. B. eine EDV-Anlage angeschlossen ist, werden Daten im Klartext an das Chiffriergerät abgegeben bzw. von diesem entgegengenommen. Entsprechend werden am Kanalanschluß **11** die chiffrierten Daten abgegeben bzw. entgegengenommen. Das Chiffriergerät muß dabei wie die EDV-Anlage gegen unbefugten Zugriff geschützt werden.

Das Chiffriergerät **12** umfaßt vorzugsweise folgende Elemente: einen Chiffriergenerator **2**, einen Schalter **3**, einen Kanalcodierer/Modulator **4**, einen Monitor **5**, einen Authentifikationsprozessor **6**, eine Eingabeeinheit **7**, eine Anzeige **8**, einen Speicher **9** und einen Zufallszahlengenerator **10**.

Der Chiffriergenerator **2** verschlüsselt den Klartext und führt den verschlüsselten Text über den Schalter **3** dem Kanalcodierer **4** zu. Dieser codiert z. B. den verschlüsselten Text damit allfällige Fehler korrigiert werden können, um die Synchronisation beim Empfänger zu erleichtern, moduliert das Signal auf die Trägerfrequenz usw. und an einen anderen, zweiten Teilnehmer B.

Der Chiffriergenerator **2** wird mit einem authentifizierten Geheimschlüssel gestartet, welcher vom Authentifikationsprozessor **6** erzeugt und abgegeben wird. Der Authentifikationsprozessor **6** ist mit der Anzeige **8** und der Eingabeeinheit **7** verbunden, mit welcher das Gerät gestartet und kontrolliert werden kann. Ferner hat der Prozessor Zugriff auf den Speicher **8** und ist an den Zufallsgenerator **10** angeschlossen.

Der gesamte Betriebsablauf wird im Monitor **5** gesteuert und überwacht. Insbesondere steuert er den Schalter **3**, über welchen wahlweise der Monitor selbst, der Authentifikationsprozessor **6** oder der Chiffriergenerator **2** an den Kanalcodierer **6** angeschlossen werden können. Daneben wirkt der Monitor auf Chiffriergenerator **2**, den Authentifikationsprozessor **6** und den Kanalcodierer **4** ein.

Das erfindungswesentliche Element des Chiffriergeräts **12** ist der Authentifikationsprozessor **6**. Er arbeitet nach dem nachstehend beschriebenen Verfahren zur Erzeugung von authentifizierten Geheimschlüsseln.

Fig. 2 zeigt eine schematische Darstellung dieses Verfahrens, welches sich groß in zwei Abschnitte aufteilen läßt, in die Präauthentifikation und den Schlüsselaufbau.

In einem Netz mit einer Anzahl Teilnehmern muß jeder zuerst die Präauthentifikation durchführen. Diese sei am Beispiel des Teilnehmers A erläutert.

Als erstes wählt A einen geeigneten endlichen Körper $GF(p)$ so daß vorzugsweise $p-1$ mindestens einen großen Primfaktor enthält und ein Element $\alpha \varepsilon GF(p)$, welches vorzugsweise primitiv ist. Ferner erzeugt er (random) eine erste Zahl

$\xi \varepsilon 0 \ldots p-2.$

Als zweites bildet er einen Authentifikationsschlüssel α^{ξ}, indem er das Element α in seinem endlichen Körper $GF(p)$ mit der ersten Zufallszahl ξ potenziert.

Und als drittes gibt er $GF(p)$, das Element α und Authentifikationsschlüssel α^{ξ} in authentifizierter Weise öffentlich bekannt. Zu diesem Zweck geht er z. B. zu einer Schlüsselzentrale und weist sich (z. B. mit einem Reisepaß) aus. Die Authentifikationszentrale trägt dann den Teilnehmer A und dessen öffentliche Daten, nämlich $GF(p)$, α, α^{ξ}, in eine öffentliche Datei (public file) ein.

Die erste geheime Zufallszahl ξ wird in einem zugriffssicheren Speicher **9** (**Fig.** 1) abgelegt und für immer geheimgehalten. Sie kann z. B. als elektronische Gerätenummer in einem Speicher abgelegt sein, welcher seinen Inhalt bei nicht autorisierten Leseversuchen zerstört.

Auf analoge Weise führen die übrigen Teilnehmer B, Cusw. die Präauthentifikation durch.

Wenn der Teilnehmer A mit dem Teilnehmer B einen gesicherten Datenaustausch beginnen will, startet er die in der Kommunikationstechnik üblichen Protokolle und erzeugt dann auf die folgende Weise einen Schlüssel.

Er besorgt sich auf authentifizierte Weise, z. B. bei seiner Authentifikationszentrale oder von den öffentlichen Daten des Teilnehmers B: $GF(q)$, β, β^{γ}.

Dann erzeugt er als erstes zufällig eine zweite Zahl

$x \varepsilon 0 \ldots q-2.$

Als zweites bildet er dann die Größe β^{x}, indem er das Element im endlichen Körper $GF(q)$ des Teilnehmers B mit seiner zweiten Zufallszahl x potenziert.

Ebenso verfährt Teilnehmer B, nachdem er erfahren hat, daß A mit ihm einen gesicherten Datenaustausch vornehmen will. Er hat also eine zweite Zufallszahl

$y \varepsilon 0 \ldots p-2$

und die Größe α^{y} erzeugt.

Als drittes tauschen A und B die Größen β^{x} und α^{y} aus und berechnen den gemeinsamen authentifizierten Geheimschlüssel

$\alpha^{\xi y} \cdot \beta^{\xi x}$

im kleinsten endlichen Körper $GF(r)$, welcher $GF(p)$ und $GF(q)$ umfaßt. Teilnehmer A kann dies über die Berechnung des Ausdruckes

$(\alpha^{y})^{\xi} (\beta^{\xi})^{x}$

und Teilnehmer B über die Berechnung von:

$(\alpha^{x})^{\gamma} (\beta^{x})^{\xi}.$

Nach dieser Schlüsselkonstruktion, die ebenso wie die Präauthentifikation im Chiffriergerät von **Fig.** 1 vom Authentifikationsprozessor **6** des jeweiligen Teilnehmers durchgeführt wird, kann der gesicherte Datenaustausch beginnen.

Ähnlich wie beim bekannten Diffie-Hellman-Verfahren kennt ein Eindringlich beim vorliegenden Verfahren nur die Größen $\alpha^{\hat{x}}$, α^{y}, $\beta^{\hat{y}}$, β^{x} was nach den heutigen Kenntnissen nicht genügt, um den Geheimschlüssel $\alpha^{\hat{x}y} \cdot \beta^{x\hat{y}}$ in angemessener Zeit zu berechnen, wenn der endliche Körper geeignet gewählt wurde. Es kann sich keiner für *A* oder *B* ausgeben, falls die Präauthentifikation korrekt durchgeführt wurde und die allenfalls vorhandene Schlüsselzentrale keine falschen Authentifikationen vornimmt. (Letzters wäre gleichbedeutend mit einer Behörde, die Paßfälschungen vornimmt.)

Schließlich bleiben selbst beim Bekanntwerden eines Identifikationscodes $\hat{x}$, $\hat{y}$ die in der Vergangenheit ausgetauschten Daten gesichert. Als einziger bekannter Angriff kann sich ein Dritter für den entsprechenden Teilnehmer während zukünftigen Schlüsselkonstruktionen ausgeben.

Eine Tatsache, die sich vor allem im Hinblick auf eine effiziente Implementierung des erfindungsgemäßen Verfahrens positiv auswirkt, ist die, daß sowohl in der Präauthentifikation als auch beim Schlüsselaufbau als aufwendige mathematische Operation nur die Exponentiation auftaucht. Gemäß einer bevorzugten Ausführungsform verwenden die Teilnehmer *A* und *B* dabei denselben endlichen Körper *GF(p)* und dieselbe Basis α.

Die Verwaltung der Authentifikationsschlüssel $\alpha^{\hat{x}}$, $\beta^{\hat{y}}$ ist sehr einfach. In einem Netz mit *M* Teilnehmern genügt eine Tabelle, deren Größe proportional zu *M* ist.

Der Identifikationscode $\hat{x}$ kann z. B. eine Art elektronische Gerätenummer sein, die z. B. in der Betriebnahme des Geräts im zugriffsgesichertem Speicher 9 abgespeichert wird. Bei dieser Gelegenheit können auch die Authentifikationsschlüssel weiterer Geräte (z. B. einer Authentifikationszentrale) installiert werden. Bei einer solchen Vorgehensweise sind nicht die Benutzer (Teilnehmer), sondern die Geräte authentifiziert, was in vielen Anwendungen das eigentliche Ziel ist.

Patentansprüche

1. Verfahren zur Erzeugung von authentifizierten Geheimschlüsseln, **dadurch gekennzeichnet,** daß in einem Netz mit Teilnehmern *A* und *B* für eine Präauthentifikation jeder Teilnehmer *A* (resp. *B)*

   a) einen endlichen Körper *GF(p)* (resp. *GF(q)*), ein Element α (resp. β) aus dem endlichen Körper *GF(p)* (resp. *GF(q))* und eine erste geheime Zufallszahl $\{\hat{x} \varepsilon 0 \ldots p-2\}$ (resp. $\{\hat{y} \varepsilon 0 \ldots q-2\}$) wählt,

   b) daß er einen Authentifikationsschlüssel $\alpha^{\hat{x}}$ (resp. $\beta^{\hat{y}}$) bildet, indem er sein Element α (resp. β) mit seiner ersten geheimen Zufallszahl $\hat{x}$ (resp. $\hat{y}$) potenziert,

   c) und daß er seinen Authentifikationsschlüssel $\alpha^{\hat{x}}$ (resp. $\beta^{\hat{y}}$) zusammen mit dem endlichen Körper *GF(p)* (resp. *GF(q))* und das Element α (resp. β) in authentifizierter Weise öffentlich bekannt gibt,

   und für einen authentifizierten Schlüsselaufbau zwischen zwei Teilnehmern *A* (resp. *B)*

   d) jeder der beiden Teilnehmer *A* und *B* eine zweite geheime Zufallszahl $\{x \varepsilon 0 \ldots q-2\}$ (resp. $\{y \varepsilon 0 \ldots p-2\}$) und

   e) einen Betriebsschlüssel β^{x} (resp. α^{y}) erzeugt, indem er das Element β (resp α) des anderen Teilnehmers *B* (resp. *A)* mit seiner zweiten geheimen Zufallszahl *x* (resp. *y)* potenziert,

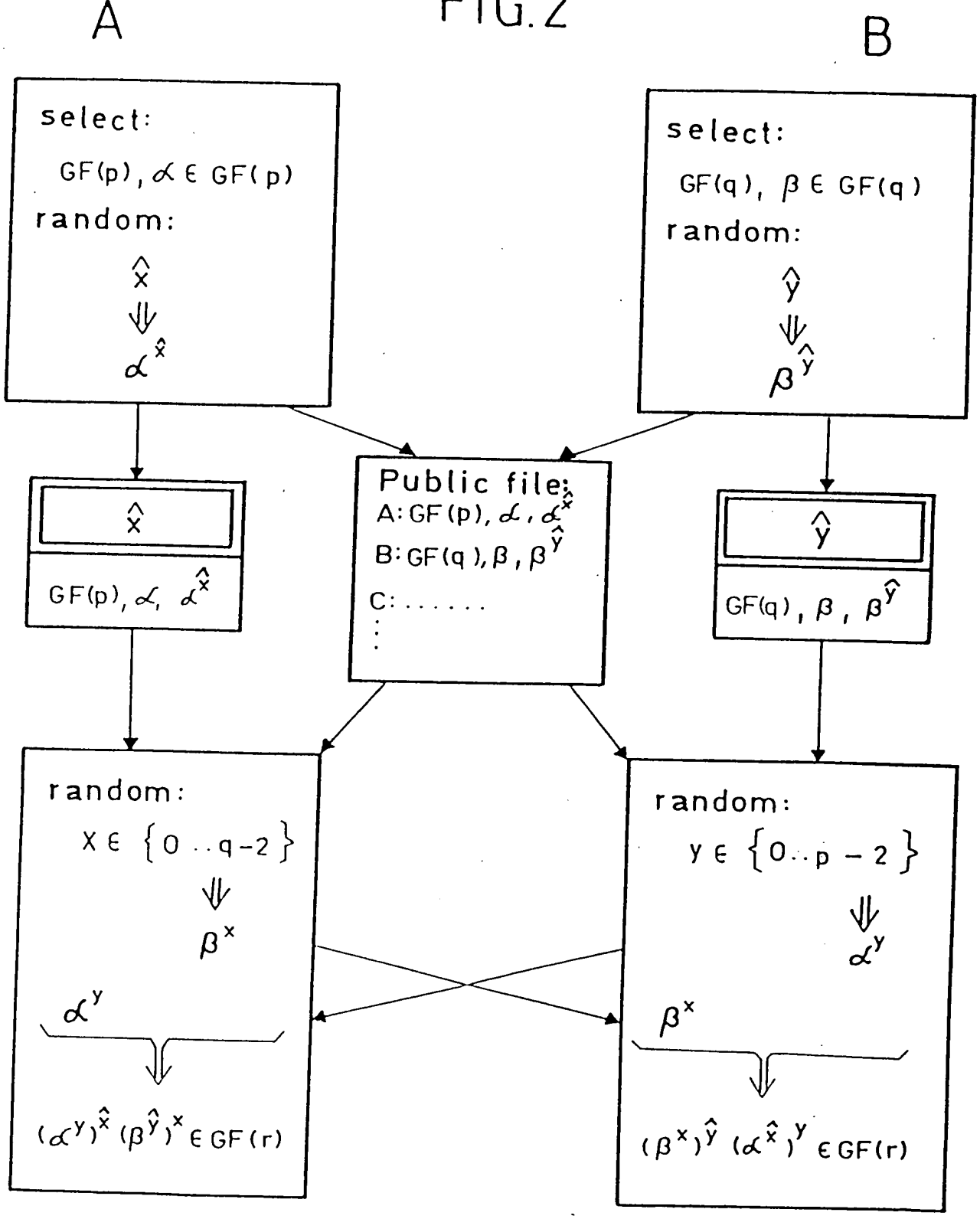
   f) und die beiden Teilnehmer *A* und *B* den gemeinsamen authentifizierten Geheimschlüssel berechnen

   $$\alpha^{\hat{x}y} \cdot \beta^{\hat{y}x}.$$

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Teilnehmer in der Präauthentifikation und beim Schlüsselaufbau denselben gemeinsamen endlichen Körper *GF(p)* verwenden.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Teilnehmer dasselbe Element (α) wählen.

FIG.2


A
B
select:
GF(p), α ∈ GF(p)
random:
x̂
α^x̂
select:
GF(q), β ∈ GF(q)
random:
ŷ
β^ŷ
Public file:
A: GF(p), α, α^x̂
B: GF(q), β, β^ŷ
C: .....
x̂
GF(p), α, α^x̂
ŷ
GF(q), β, β^ŷ
random:
X ∈ {0 .. q-2}
β^x
α^y
(α^y)^x̂ (β^ŷ)^x ∈ GF(r)
random:
y ∈ {0 .. p-2}
α^y
β^x
(β^x)^ŷ (α^x̂)^y ∈ GF(r)

Offenlegungstag: 30. November 1989

11

3915262

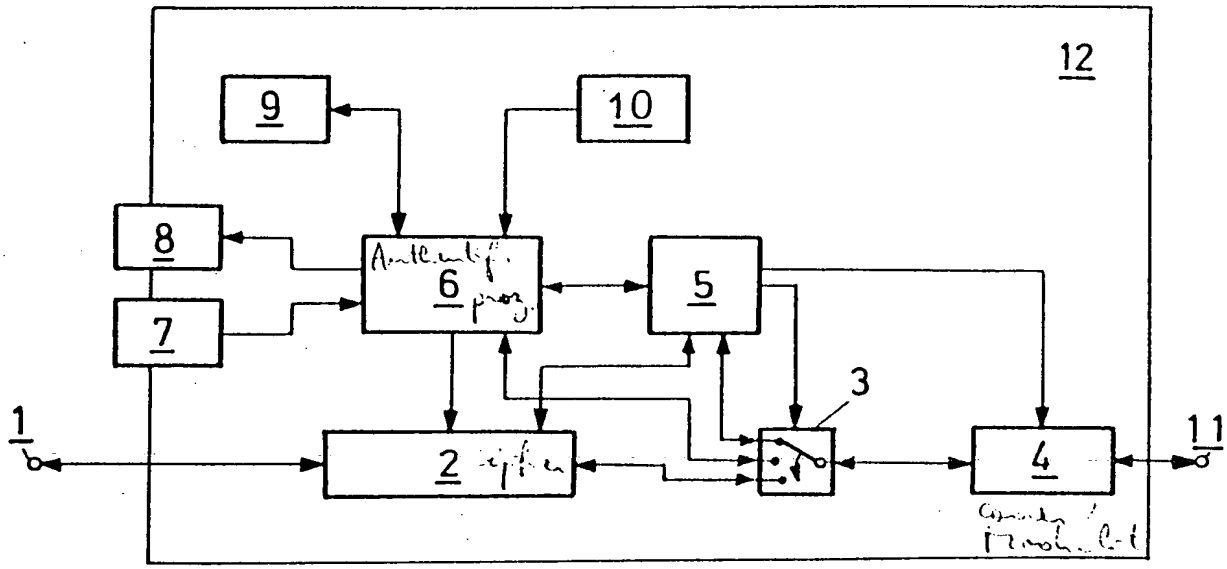


FIG.1